

AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1. (Currently Amended) A method, comprising:

generating by a first apparatus which controls access to a low power radio communications network a shared secret at the first apparatus and storing the shared secret in a memory of the first apparatus, wherein the stored secret is associated with an operational mode of the first apparatus where a user of the first apparatus is not to be interrupted and where the stored secret is used for automatic pairing when the first apparatus is in the operational mode;

making the stored shared secret available at a second apparatus;

receiving a signal from the second apparatus to initiate a pairing process with the first apparatus on the low power radio communications network, where the signal comprises a request to pair with the first apparatus for a required service from the first apparatus;

determining whether the first apparatus is in the operational mode where the user of the first apparatus is not to be interrupted and whether the required service is associated with the stored shared secret; and

for the case where it is determined that the first apparatus is in the operational mode where the user of the first apparatus is not to be interrupted and the required service is associated with the stored shared secret, then initiating the ~~automatic~~

pairing process, automatically with no intervention from the user of the first apparatus, using the stored shared secret or else

prompting the user of the first apparatus to enter a shared secret associated with the requested service and initiating the pairing process using the user entered shared secret.

2. (Currently Amended) The method as claimed in claim 1, where the initiated pairing process comprises an algorithm that uses one of the stored shared secret and the shared secret entered by the user as an input to the algorithm.
3. (Currently Amended) The method as claimed in claim 1, further comprising, based on the initiated pairing process, establishing the communication with the second apparatus and providing the requested service to the second apparatus.
4. (Previously Presented) The method as claimed in claim 1, wherein the determined operational mode comprises a gaming mode.
5. (Previously Presented) The method as claimed in claim 1, further comprising, selecting the operational modes in which the user of the first apparatus is not to be interrupted.
6. (Previously Presented) The method as claimed in claim 1, where the required service comprises a gaming service.
7. (Previously Presented) The method as claimed in claim 1, wherein making the stored shared secret available at the second apparatus involves prompting a user input of the shared secret at the second apparatus.
8. (Previously Presented) The method as claimed in claim 1 where the shared secret comprises a secret PIN.

9. (Currently Amended) The method as claimed in claim 2, wherein the algorithm creates a secret key for use in the pairing process and where the secret key uses a random number communicated between the first apparatus and the second apparatus.

10. (Previously Presented) The method as claimed in claim 9, wherein the algorithm creating the secret key uses an identifier of one of the first apparatus and the second apparatus, communicated between the first apparatus and the second apparatus, in the creation of the secret key.

11. (Previously Presented) The method as claimed in claim 1, further comprising: re-using the stored shared secret to join a third apparatus to the low power radio communications network without contemporaneous user input of the shared secret at the first apparatus, comprising: making the stored shared secret available at the third apparatus; and

creating in the first apparatus, using the shared secret, a secret key; and making the secret key available to the third apparatus for use in pairing the third apparatus and the first apparatus to secure communication between them.

12. (Currently Amended) A method, comprising:

receive at a second apparatus of a low power radio communications network a shared secret;

sending a signal to a first apparatus to initiate a pairing process in the low power radio communications network with the first apparatus, where the signal comprises a request to pair with the first apparatus for a required service from the first apparatus, where the signal to initiate the pairing process prompts the first apparatus to determine whether the first apparatus is in an operational mode where a user of the first apparatus is not to be interrupted and whether the required service is associated with a shared secret stored on the first apparatus for use in automatic pairing when the first apparatus is in the operational mode; and

for the case where it is determined that the first apparatus is in the operational mode where the user of the first apparatus is not to be interrupted and the required service is associated with the shared secret stored on the first apparatus, then receiving an acceptance message from the first apparatus and inputting, at the second apparatus, the shared secret received at the second apparatus for the pairing process, where the pairing process is initiated automatically on the first apparatus with no intervention from the user of the first apparatus, using the shared secret stored on the first apparatus, or else

the signal to initiate the pairing process prompts the user of the first apparatus to enter a shared secret associated with the requested service for the pairing process.

13. (Currently Amended) The method as claimed in claim 12, where the initiated pairing process comprises an algorithm that uses one of the stored shared secret and the shared secret entered by the user of the first apparatus as an input to the algorithm.

14. (Currently Amended) An apparatus comprising:

at least one processor; and

at least one memory including computer readable instructions, where the at least one memory and the computer readable instructions are configured, with the at least one processor, to cause the apparatus to at least:

store a shared secret for use in securing communications in a low power radio communications network comprising the apparatus and one or more additional apparatus, wherein the stored shared secret is associated with an operational mode of the apparatus where a user of the apparatus is not to be interrupted and where the stored secret is used for automatic pairing when the apparatus is in the operational mode;

communicate in the network and receive a signal from the one or more additional apparatus to initiate a pairing process with the apparatus on the low power communications network, where the signal comprises a request to pair with the apparatus for a required service from the apparatus;

determine whether the apparatus is in an operational mode where the user of the apparatus is not to be interrupted and whether the required service is associated with the stored shared secret; and

for the case where it is determined that the apparatus is in the operational mode where the user of the apparatus is not to be interrupted and the required service is associated with the stored shared secret, initiate the automatic pairing process, automatically with no intervention from the user of the apparatus, using the stored shared secret, or else

prompt the user of the apparatus to enter a secret associated with the requested service and initiate the pairing process using the user entered shared secret.

15. (Currently Amended) The apparatus as claimed in claim 14, where the initiated pairing process comprises an algorithm that uses one of the stored secret and the secret entered by the user as an input to the algorithm.

16. (Previously Presented) The apparatus as claimed in claim 14, wherein the operational mode comprises a game mode.

17. (Previously Presented) The apparatus as claimed in claim 14, wherein the required service comprises a gaming service.

18. (Currently Amended) The apparatus as claimed in claim 14, comprising the apparatus

is caused, in response to the determining, to access the secret in the memory to create a secret key for use in the pairing process without user intervention.

19. (Previously Presented) The apparatus as claimed in claim 18, wherein the apparatus is caused to automatically create the secret key in response to the received signal.

20. (Previously Presented) The apparatus as claimed in claim 14, wherein the stored shared secret is independent of an origin of the received signal.

21. (Previously Presented) The apparatus as claimed in claim 18, wherein the secret key is dependent upon an origin of the received signal.

22. (Previously Presented) The apparatus as claimed in claim 18, wherein the secret key is dependent upon content of the received request.

23. (Previously Presented) The apparatus as claimed in claim 22, wherein the request includes a random value used with at least the stored shared secret to create the secret key.

24. (Previously Presented) The apparatus as claimed in claim 14, wherein the apparatus is caused, in a first mode, to obtain a secret by accessing the shared secret stored in the memory, in a second mode, to obtain a shared secret by enabling user input of data, and in the first mode and in the second mode, to create, using the obtained shared secret, the secret key for use in pairing the apparatus and the one or more additional apparatus to secure communication between them.

25. (Previously Presented) The apparatus as claimed in claim 24, wherein the first mode is an interactive gaming mode and second mode is an idle mode.

26. (Previously Presented) The apparatus as claimed in claim 14, wherein the apparatus is caused to store an apparatus identifier for use with at least the stored shared secret to create the

secret key.

27. (Previously Presented) The apparatus as claimed in claim 15, further comprising the apparatus is caused to program the value of the stored shared secret.

28. (Previously Presented) The apparatus as claimed in claim 14, wherein the secret key is for use in securing all communications in the network.

29. (Currently Amended) The memory embodying instructions executable by a processor of claim 35, where initiating the pairing process comprises using an algorithm and where the algorithm uses one of the stored shared secret and the shared secret entered by the user as an input to the algorithm.

30. (Previously Presented) The apparatus as claimed in claim 14, further comprising the apparatus is caused, when the apparatus participates in a different network controlled by a different apparatus, to enter a shared secret stored at the different apparatus and to create, using the entered shared secret, a secret key for securing communication.

31.-33. (Canceled)

34. (Currently Amended) An apparatus comprising:

at least one processor; and

at least one memory including computer readable instructions, where the at least one memory and the computer readable instructions are configured, with the at least one processor, to cause the apparatus to at least:

communicate on a low power radio communications network;

receive at the apparatus a shared secret for use in securing communications in the low power radio communications network;

send a signal to a device to initiate a pairing process in the low power communications network with the device, where the signal comprises a request to pair with the device for a required service from the device, where the signal to initiate the pairing process prompts the device to determine whether the device is in an operational mode where a user of the device is not to be interrupted and whether the required service is associated with a stored shared secret on the device for use in automatic pairing when the device is in the operational mode; and

for the case where it is determined that the device is in the operational mode where the user of the device is not to be interrupted and the required service is associated with the shared secret stored on the device, then receiving an acceptance message from the device and inputting, at the apparatus, the shared secret received at the apparatus for the pairing process, where the pairing process is initiated automatically on the device with no intervention from the user of the device, using the shared secret stored on the device, or else

the signal to initiate the pairing process prompts the user of the device to enter a shared secret associated with the requested service for the initiated pairing process.

35. (Currently Amended) A memory embodying a program of computer readable instructions that when executed by a processor perform actions directed to securing communication between a first and second apparatus, the actions comprising:

generating a shared secret at the first apparatus which controls access to a low power radio communications network and storing the shared secret in a memory of the first apparatus, wherein the stored shared secret is associated with an operational mode of the first apparatus where a user of the first apparatus is not to be interrupted and where the stored shared secret is used for automatic pairing when the first apparatus is in the operational mode;

making the stored shared secret available at the second apparatus;

receiving a signal from the second apparatus to initiate a pairing process with the first apparatus on the low power radio communications network, where the signal comprises a request to pair with the first apparatus for a required service from the first apparatus;

determining whether the first apparatus is in an operational mode where the user of the first apparatus is not to be interrupted and whether the required service is associated with the stored shared secret; and

for the case where it is determined that the first apparatus is in the operational mode where the user of the first apparatus is not to be interrupted and the required service is associated with the stored shared secret then initiating the automatic pairing process, automatically with no intervention from the user of the first apparatus, using the stored shared secret, or else

prompting the user of the first apparatus to enter a shared secret associated with the requested service and initiate the pairing process with the second apparatus using the user entered shared secret.

36. (Previously Presented) The memory embodying instructions executable by a processor of claim 35, wherein the operational mode comprises a game mode.

37. (Currently Amended) The apparatus as claimed in claim 34 where initiating the pairing process comprises using an algorithm and where the algorithm uses one of the stored shared secret and the shared secret entered by the user of the device as an input to the algorithm.